



Azure Compute Migration/Network #2

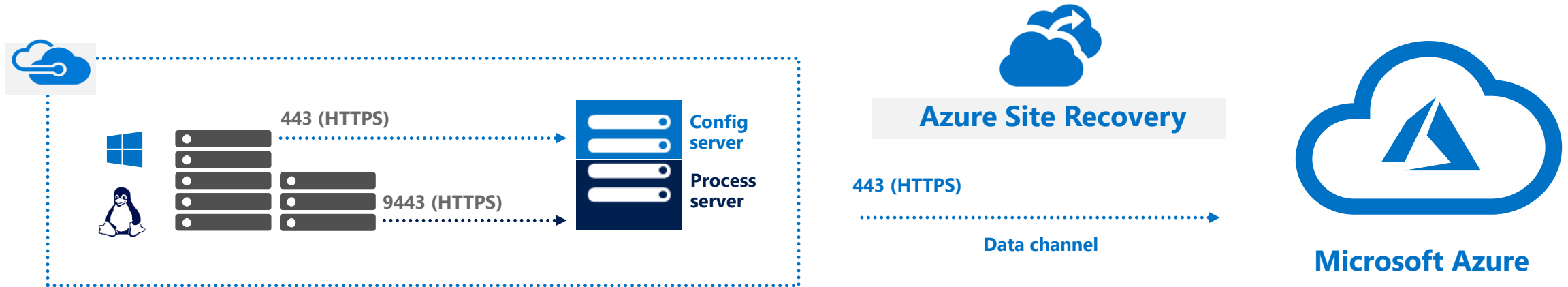
한국마이크로소프트 조민애

Agenda

- Azure 재해 복구 서비스
- Azure 가상 네트워크 라우팅
- Azure 부하 분산 관련 서비스
 - Azure 부하 분산기
 - 트래픽 관리자
 - Azure 애플리케이션 게이트웨이
- Azure Firewall

Azure 재해 복구 서비스

- Azure 재해 복구 서비스(Azure Site Recovery)를 이용하여 온-프레미스에 있는 인프라를 Azure로 안전하게 복제할 수 있습니다.



Source: VMware VMs and physical servers

Public internet or ExpressRoute with public peering

Azure 재해 복구 서비스

1. Source 위치

- VMWare
- Hyper-V
- Physical
- Azure VM

Question :

UEFI Boot?

Windows 2003?

vCenter server and vSphere support	6.5, 6.0, 5.5	
Windows guest OS support	Windows Server 2016 Windows Server 2012 R2	Windows Server 2012 Windows Server 2008 R2
Linux guest OS support	RHEL 5.*, 6.* and 7.* Cent OS 5.*, 6.* and 7.* Ubuntu 14.04 and 16.04 LTS	SUSE Enterprise Server 11 SP3, SP4 OEL 6.4 and 6.5 Debian 7 and 8 support
Azure platform support	Managed disk Up to 4TB data disk support	Encrypted storage Azure Hybrid benefit

Azure 재해 복구 서비스

2. 구성 서버 – 온-프레미스와 Azure 간 통신 조정. 데이터 복제 관리



CPU	메모리	캐시 디스크	데이터 변경률	복제될 컴퓨터
vCPU 8대 2개 소켓*4코어 @2.5GHz	16GB	300GB	500GB 이하	100대 미만
vCPU 12대 2개 소켓 * 6코어 @ 2.5GHz	18GB	600GB	500GB-1TB	100-150대
vCPU 16대 2개 소켓* 8코어 @ 2.5GHz	32GB	1TB	1-2TB	150-200대

온-프레미스 사이트 or Azure상 구축 가능

Azure 재해 복구 서비스

3. Azure

Blob 스토리지 – VHD 저장

Azure Recovery Service 자격 증명

Azure 네트워크



Azure 재해 복구 서비스 – Azure 포털 화면

Azure 준비

- 스토리지 계정
- Recovery Services 자격 증명 모음
- Azure 네트워크

The screenshot shows the 'Create storage account' page in the Azure portal. The left sidebar contains a navigation menu with options like Dashboard, Recent, Subscriptions, All resources, Application gateways, DNS zones, Load balancers, Network interfaces, Public IP addresses, Network security groups, Resource groups, Security Center, Storage accounts, Traffic Manager profiles, Virtual machines, Virtual network gateways, and Virtual networks. The main content area is titled 'Create storage account' and includes a 'Report a bug' button. Below the title, there is a note about the cost of the storage account. The form fields include: Name (contosovmsacct1910171607), Deployment model (Resource manager), Account kind (General purpose), Performance (Standard), Replication (Read-access geo-redundant storage (R...)), Secure transfer required (Disabled), Subscription (Microsoft Azure Internal Consumption), Resource group (ContosoRG), and Location (West Europe). There is a 'Pin to dashboard' checkbox and a 'Create' button at the bottom.

Azure 재해 복구 서비스 – Azure 포털 화면

Azure 준비

- 스토리지 계정
- Recovery Services 자격 증명 모음
- Azure 네트워크

Recovery Services vault

Recovery Services vault

*

Name

ContosoVMVault

✓

*

Subscription

Contoso Subscription

▼

*

Resource group

☐ Create new

☒ Use existing

contosoRG

▼

*

Location

West Europe

▼

☒ Pin to dashboard

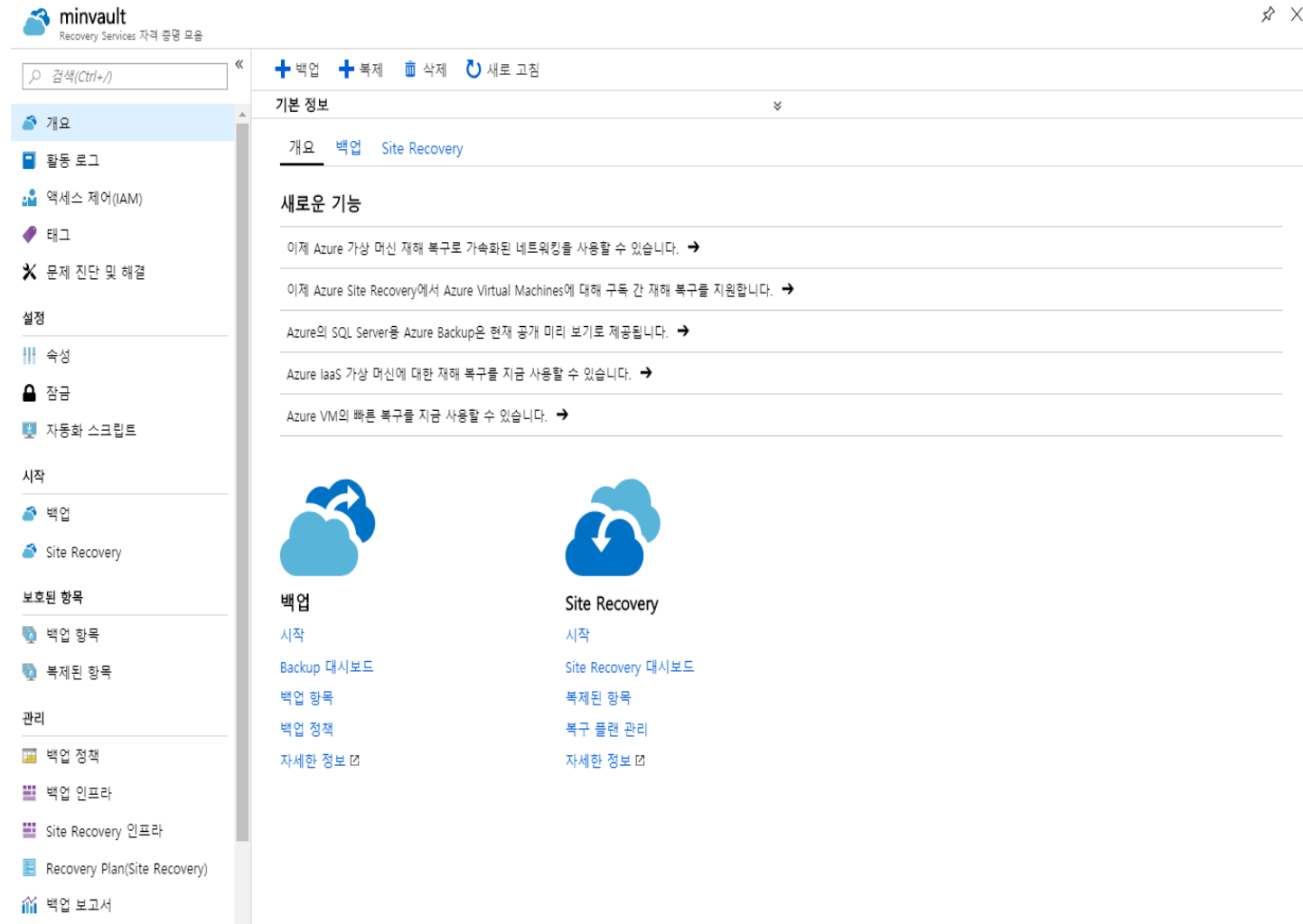
Create

Automation options

Azure 재해 복구 서비스 – Azure 포털 화면

Azure 준비

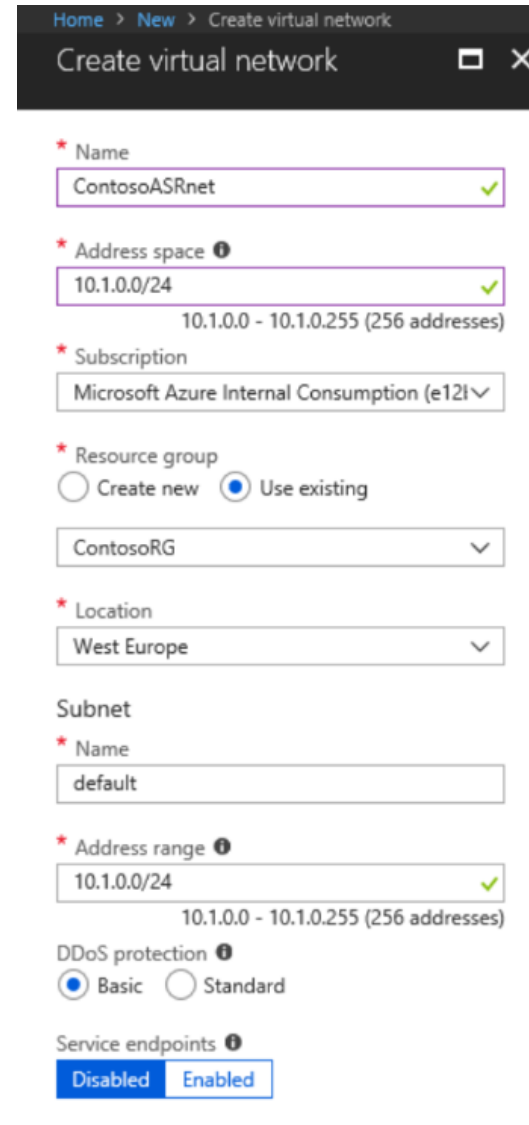
- 스토리지 계정
- Recovery Services 자격 증명 모음
- Azure 네트워크



Azure 재해 복구 서비스 – Azure 포털 화면

Azure 준비

- 스토리지 계정
- Recovery Services 자격 증명 모음
- Azure 네트워크



The screenshot shows the 'Create virtual network' form in the Azure portal. The form is titled 'Create virtual network' and has a breadcrumb trail 'Home > New > Create virtual network'. The form contains the following fields and options:

- Name:** ContosoASRnet (with a green checkmark)
- Address space:** 10.1.0.0/24 (with a green checkmark). Below the input, it says '10.1.0.0 - 10.1.0.255 (256 addresses)'.
- Subscription:** Microsoft Azure Internal Consumption (e12l) (with a dropdown arrow)
- Resource group:** ContosoRG (with a dropdown arrow). The options are 'Create new' (radio button) and 'Use existing' (radio button, selected).
- Location:** West Europe (with a dropdown arrow)
- Subnet:**
 - Name:** default (with a dropdown arrow)
 - Address range:** 10.1.0.0/24 (with a green checkmark). Below the input, it says '10.1.0.0 - 10.1.0.255 (256 addresses)'.
- DDoS protection:** Basic (radio button, selected) or Standard (radio button).
- Service endpoints:** Disabled (button) or Enabled (button).

Azure 재해 복구 서비스 – Azure 포털 화면

온-프레미스 준비

- 구성. 프로세스 서버 준비
- 원본 서버 준비

minivault - Site Recovery 인프라

Recovery Services 자격 증명 모음

검색(Ctrl+/)

개요

활동 로그

액세스 제어(IAM)

태그

문제 진단 및 해결

설정

속성

잠금

자동화 스크립트

시작

백업

Site Recovery

보호된 항목

백업 항목

복제된 항목

관리

백업 정책

백업 인프라

Site Recovery 인프라

Recovery Plan(Site Recovery)

백업 보고서

필터 설정

AZURE 가상 머신

네트워크 매핑

복제 정책

확장 업데이트 설정

SYSTEM CENTER VMM에 대해

VMM 서버

네트워크 매핑

복제 정책

VMWARE 및 물리적 서버에 대해

Configuration Servers

복제 정책

HYPER-V 사이트에 대해

Hyper-V 사이트

Hyper-V 호스트

복제 정책

서버

minivault

+ 서버

서버에서 데이터 로드를 완료했습니다.

항목 필터링...

서버 이름	연결 상태	마지막 하트비트	에이전트 버전	서버 유형
-------	-------	----------	---------	-------

서버가 아직 등록되지 않았습니다. 시작하는 방법에 대해 자세히 알아보려면 [+ 서버]를 클릭하세요.

서버 추가

minivault

서버 유형

VMware 구성 서버

구성 서버 추가에는 15~30분 걸릴 수 있습니다.

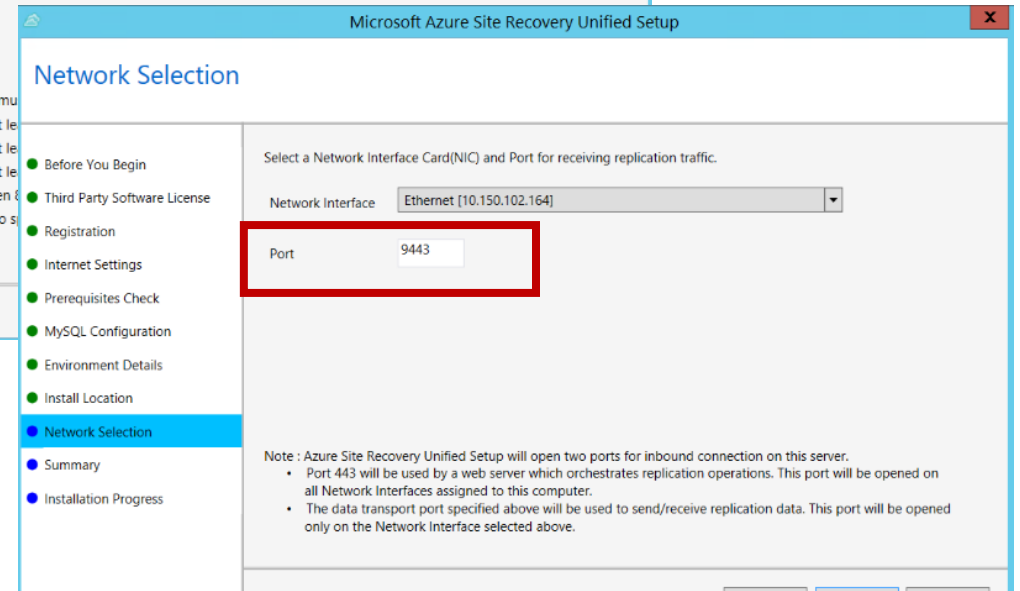
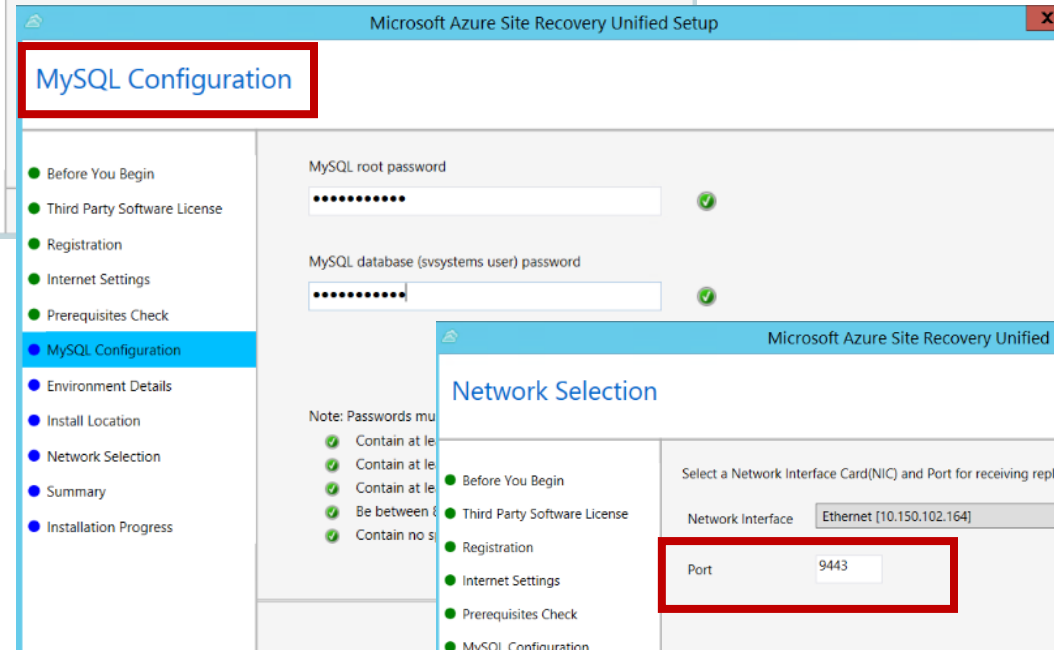
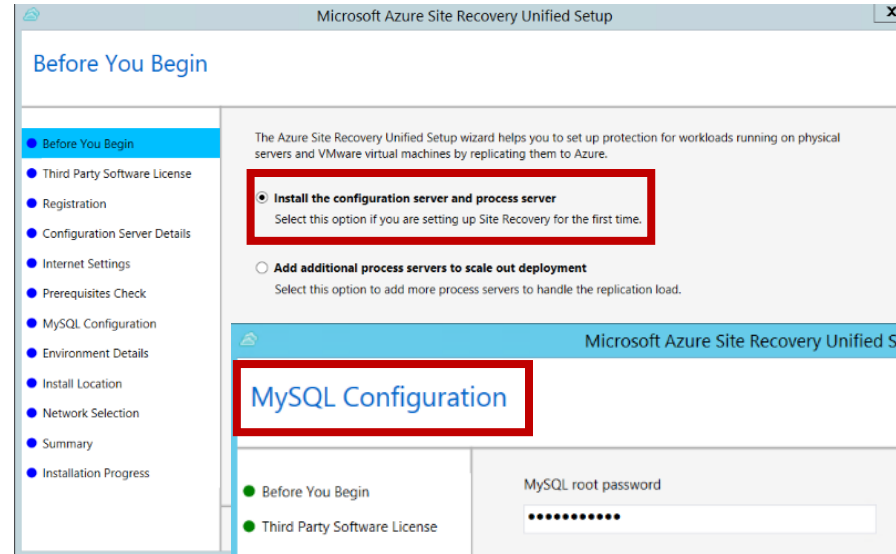
구성 서버 등록 온-프레미스

1. 다운로드 구성 서버 가상 머신 템플릿인 [vCenter](#)에 액세스할 수 있는지 확인합니다.
2. OVF 템플릿 배포 방법을 사용하여 구성 서버 가상 머신 템플릿을 vCenter 서버로 가져옵니다.
3. 부팅되면 가상 머신의 콘솔에 연결합니다.
4. 사용권 계약에 동의하고 관리자 계정을 설정하여 Windows Server 설치를 완료합니다.
5. Windows 설치가 완료되면 [VMware PowerCLI 6.0](#)을 구성 서버에 설치합니다.
6. Azure Site Recovery 구성 관리자 마법사를 시작하고 단계에 따라 Azure Site Recovery에 구성 서버를 등록합니다. [추가 정보](#)

Azure 재해 복구 서비스 – Azure 포털 화면

온-프레미스 준비

- 구성. 프로세스 서버 준비
- 원본 서버 준비



Azure 재해 복구 서비스 – Azure 포털 화면

온-프레미스 준비

- 구성 프로세스 서버 준비
- 원본 서버 준비

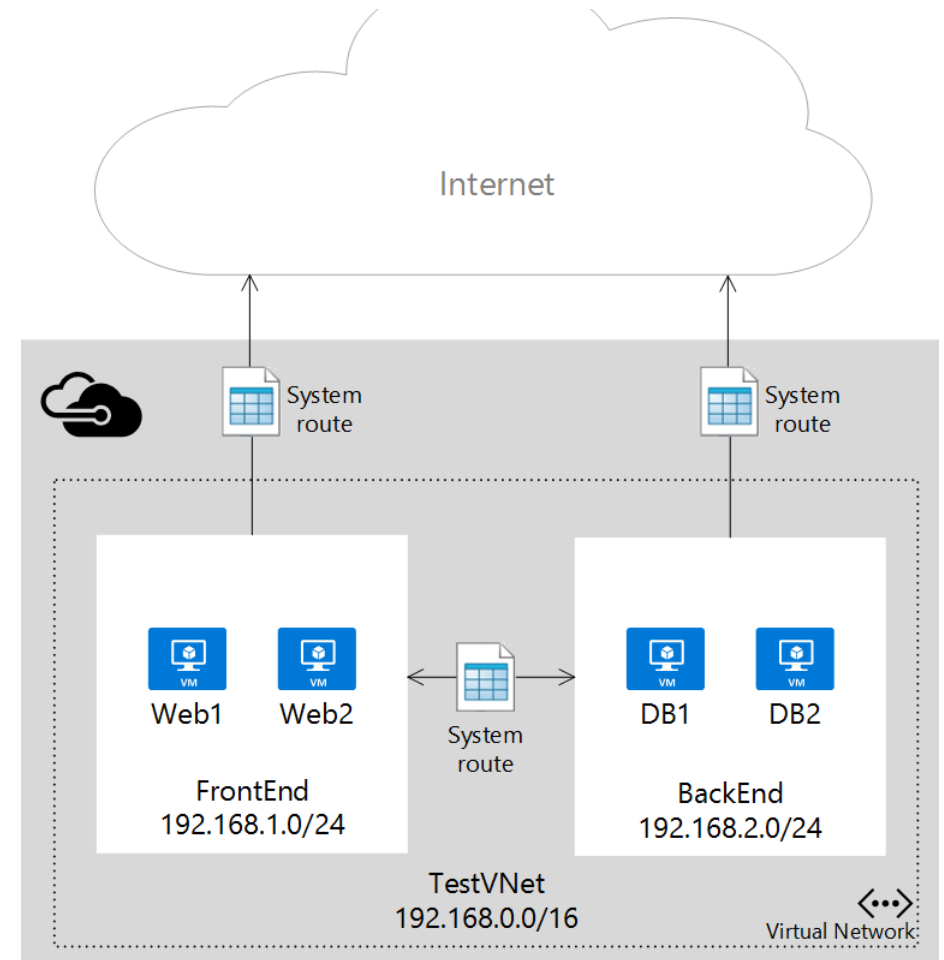
설치 관리자 파일

표에서는 각 VMware VM 및 물리적 서버 운영 체제에 대한 설치 관리자 파일을 요약합니다. 시작하기 전에 [지원되는 운영 체제](#)를 검토할 수 있습니다.

설치 관리자 파일	운영 체제(64비트만 해당)
Microsoft-ASR-UA*Windows*release.exe	Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2 SP1
Microsoft-ASR-UA*RHEL6-64*release.tar.gz	RHEL(Red Hat Enterprise Linux) 6.* CentOS 6.*
Microsoft-ASR-UA*RHEL7-64*release.tar.gz	RHEL(Red Hat Enterprise Linux) 7.* CentOS 7.*
Microsoft-ASR-UA*SLES12-64*release.tar.gz	SUSE Linux Enterprise Server 12 SP1, SP2, SP3
Microsoft-ASR-UA*SLES11-SP3-64*release.tar.gz	SUSE Linux Enterprise Server 11 SP3
Microsoft-ASR-UA*SLES11-SP4-64*release.tar.gz	SUSE Linux Enterprise Server 11 SP4
Microsoft-ASR-UA*OL6-64*release.tar.gz	Oracle Enterprise Linux 6.4, 6.5
Microsoft-ASR-UA*UBUNTU-14.04-64*release.tar.gz	Ubuntu Linux 14.04
Microsoft-ASR-UA*UBUNTU-16.04-64*release.tar.gz	Ubuntu Linux 16.04 LTS 서버
Microsoft-ASR-UA*DEBIAN7-64*release.tar.gz	Debian 7
Microsoft-ASR-UA*DEBIAN8-64*release.tar.gz	Debian 8

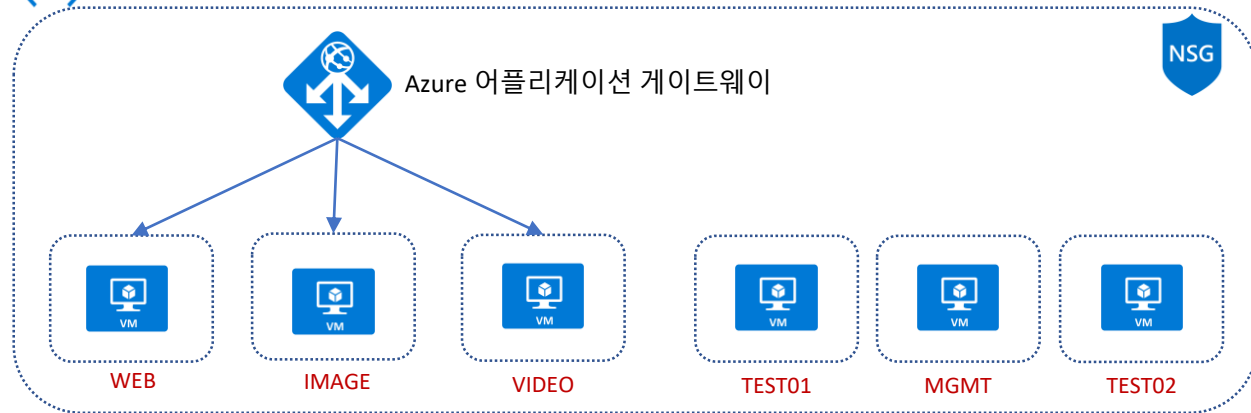
Azure 가상 네트워크

- 가상 네트워크(Virtual Network)
 - 기본적으로 서브넷간 모두 라우팅 가능
 - 네트워크 보안 그룹(NSG)을 통해 교신 제어
- 다양한 연결 방법
 - 온-프레미스와 연결
 - Azure 상의 연결
 - VNET Peering
 - Global Peering
 - VNET to VNET

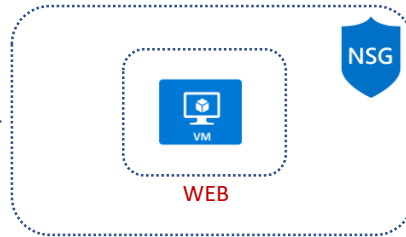


Azure 가상 네트워크

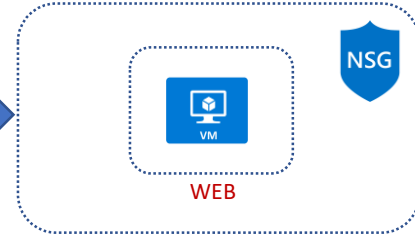
<...> 한국 중부 10.5.0.0/16



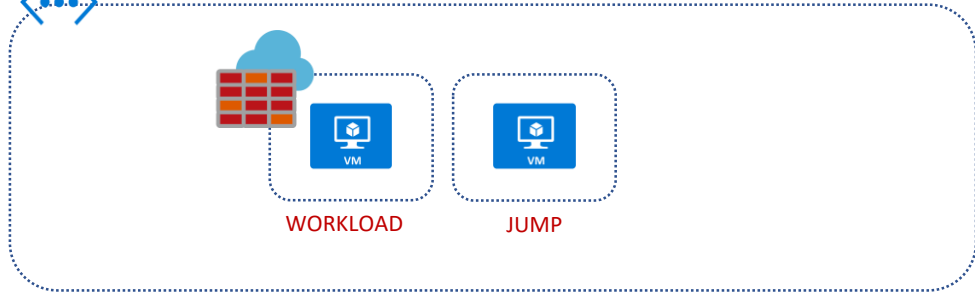
<...> 일본 동부 10.6.0.0/16



<...> 동아시아 10.7.0.0/16



<...> 한국 남부 10.11.0.0/16



Azure 가상 네트워크

- VNET Peering

Azure내 가상 네트워크를 연결하는 방법 (다른 구독 가능)
가상 네트워크 간의 트래픽이 Microsoft 백본 네트워크에서 유지됨.

인바운드 보안 규칙

우선 순위	이름	포트	프로토콜	소스	대상 주소	작업	
65000	AllowVnetInBound	모두	모두	VirtualNetwork	VirtualNetwork	✓ 허용	...
65001	AllowAzureLoadBalancerInBo...	모두	모두	AzureLoadBala...	모두	✓ 허용	...
65500	DenyAllInBound	모두	모두	모두	모두	✗ 거부	...

아웃바운드 보안 규칙

우선 순위	이름	포트	프로토콜	소스	대상 주소	작업	
65000	AllowVnetOutBound	모두	모두	VirtualNetwork	VirtualNetwork	✓ 허용	...
65001	AllowInternetOutBound	모두	모두	모두	Internet	✓ 허용	...
65500	DenyAllOutBound	모두	모두	모두	모두	✗ 거부	...

```
C:\Users\minuser01>tracert 10.5.13.4

Tracing route to 10.5.13.4 over a maximum of 30 hops

  1      1 ms      <1 ms      <1 ms    10.5.13.4

Trace complete.
```

기본적인 네트워크 보안 그룹 설정
설정을 이용한 제어 가능

Azure 가상 네트워크 – 예제 1

- VNET Peering
 - A 10.5.11.0/24
 - B-MGMT 10.5.12.0/24
 - C 10.5.13.0/24

Azure는 기본적으로 같은 가상 네트워크내 서브넷간에는 모두 라우팅이 된다고 했는데..

A<->C로의 직접 연결이 아닌..

Q. 무조건 B를 거치는 네트워크를 만들고 싶다면..?

A. 경로 테이블(Route Table)과 IP 전달(IP Forwarding)과 라우터 설정

Azure 가상 네트워크 – 예제 1

- 경로 테이블(Route Table)과 다수 NIC(Multi NIC)과 라우터 (X)

중간 MGMT 대역을 거치지 않고 바로 전송 됨

```
C:\Users\minuser01>tracert 10.5.13.4
Tracing route to 10.5.13.4 over a maximum of 30 hops
  1    <1 ms    <1 ms    <1 ms  10.5.13.4
Trace complete.
C:\Users\minuser01>_
```

Azure 가상 네트워크 – 예제 1

- 경로 테이블 설정

대시보드 > KC-PT-RG > KC-PT-RT - 경로

KC-PT-RT - 경로

경로 테이블

검색(Ctrl+/)

+ 추가

경로 검색

이름	주소 접두사	다음 홉
MGMT-RULE	10.5.13.0/24	10.5.12.4

- IP 전달

대시보드 > KC-MGMT01 - 네트워킹 > kc-mgmt01941 - IP 구성

kc-mgmt01941 - IP 구성

네트워크 인터페이스

검색(Ctrl+/)

+ 추가 저장 취소

IP 전달 설정

IP 전달

가상 네트워크

IP 구성

* 서브넷

SUBNET-MGMT(10.5.12.0/24)

IP 구성 검색

이름	IP 버전	형식	개인 IP 주소	공용 IP 주소
ipconfig1	IPv4	기본	10.5.12.4(동적)	52.231.72.157(PIP-KC-MGMT01)

Azure 가상 네트워크 – 예제 1

- 라우터 설정
 - 운영 체제내에서 IP 전달을 사용하도록 설정
 - RRAS 혹은 다른 프로그램 사용 가능

PowerShell

복사

```
Set-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters -Name IpEnableRouter -Value 1
```

- 라우팅 결과

```
C:\Users\minuser01>tracert 10.5.13.4
Tracing route to 10.5.13.4 over a maximum of 30 hops
  1      1 ms      <1 ms      <1 ms  10.5.12.4
  2      <1 ms      1 ms      <1 ms  10.5.13.4
Trace complete.
C:\Users\minuser01>_
```


가상 네트워크 라우팅

DEMO 1

Azure 가상 네트워크 – 예제 2

- 온-프레미스와 VNET Peering

- A 한국 중부



S2S. 해당 데모에서는 VNET to VNET으로 대체

- B 일본 동부



VNET Peering

- C 일본 동부

Q. 한국 중부에서 직접적으로 연결하지 않은 일본 동부의 가상 네트워크 C에 접근하려면..?

A. 게이트웨이 전송, 원격 게이트웨이 전송 허용

Azure 가상 네트워크 – 예제 2

게이트웨이 전송, 원격 게이트웨이 전송 허용 (X)

- A 한국 중부



- B 일본 동부



- C 일본 동부

```
C:\windows\system32>ping 10.6.0.4

Pinging 10.6.0.4 with 32 bytes of data:
Reply from 10.6.0.4: bytes=32 time=37ms TTL=126
Reply from 10.6.0.4: bytes=32 time=36ms TTL=126
Reply from 10.6.0.4: bytes=32 time=36ms TTL=126
Reply from 10.6.0.4: bytes=32 time=36ms TTL=126

Ping statistics for 10.6.0.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 36ms, Maximum = 37ms, Average = 36ms

C:\windows\system32>ping 10.8.1.4

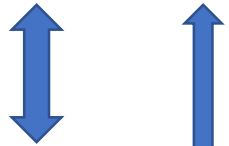
Pinging 10.8.1.4 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.8.1.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Azure 가상 네트워크 – 예제 2

게이트웨이 전송, 원격 게이트웨이 전송 허용 (O)

- A 한국 중부



- B 일본 동부



- C 일본 동부

```
C:\windows\system32>ping 10.6.0.4

Pinging 10.6.0.4 with 32 bytes of data:
Reply from 10.6.0.4: bytes=32 time=37ms TTL=126
Reply from 10.6.0.4: bytes=32 time=37ms TTL=126
Reply from 10.6.0.4: bytes=32 time=37ms TTL=126
Reply from 10.6.0.4: bytes=32 time=36ms TTL=126

Ping statistics for 10.6.0.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 36ms, Maximum = 37ms, Average = 36ms

C:\windows\system32>ping 10.8.1.4

Pinging 10.8.1.4 with 32 bytes of data:
Reply from 10.8.1.4: bytes=32 time=37ms TTL=126
Reply from 10.8.1.4: bytes=32 time=36ms TTL=126
Reply from 10.8.1.4: bytes=32 time=36ms TTL=126
Reply from 10.8.1.4: bytes=32 time=36ms TTL=126

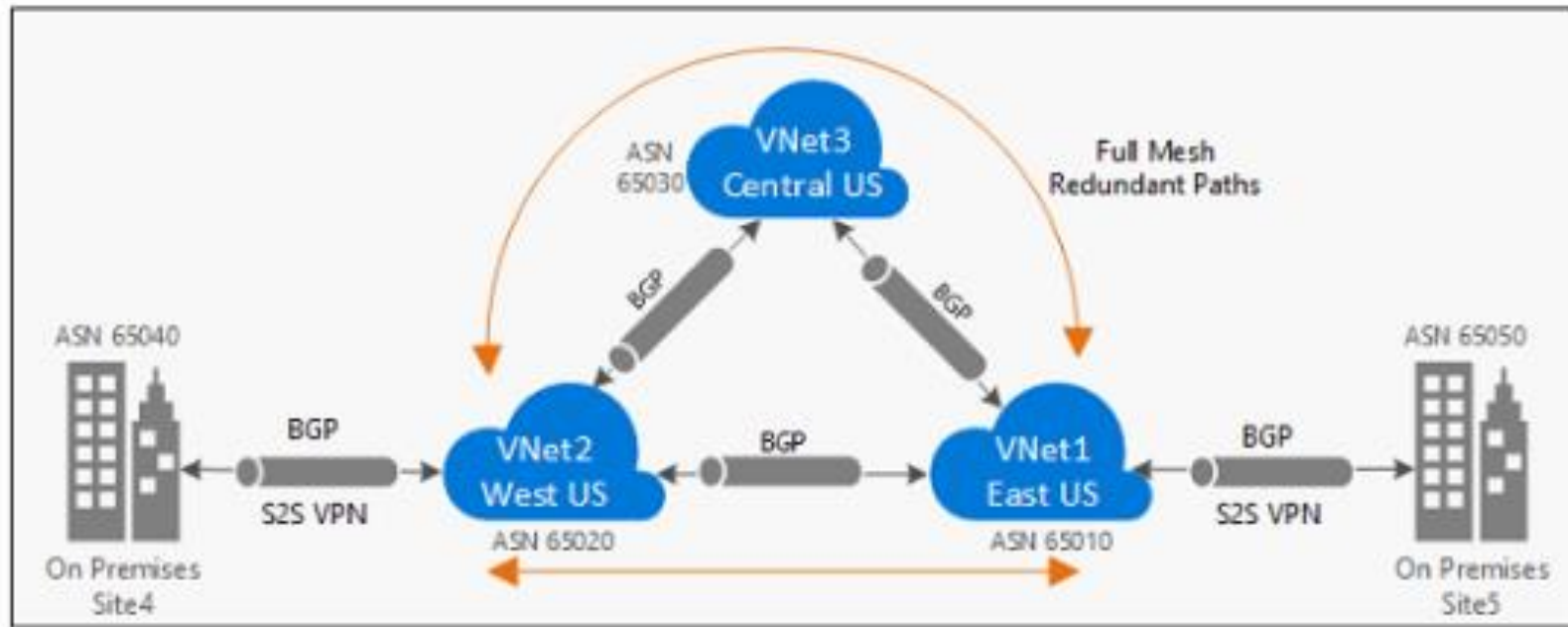
Ping statistics for 10.8.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 36ms, Maximum = 37ms, Average = 36ms
```

가상 네트워크 라우팅

DEMO 2

Azure 가상 네트워크 – 예제 3

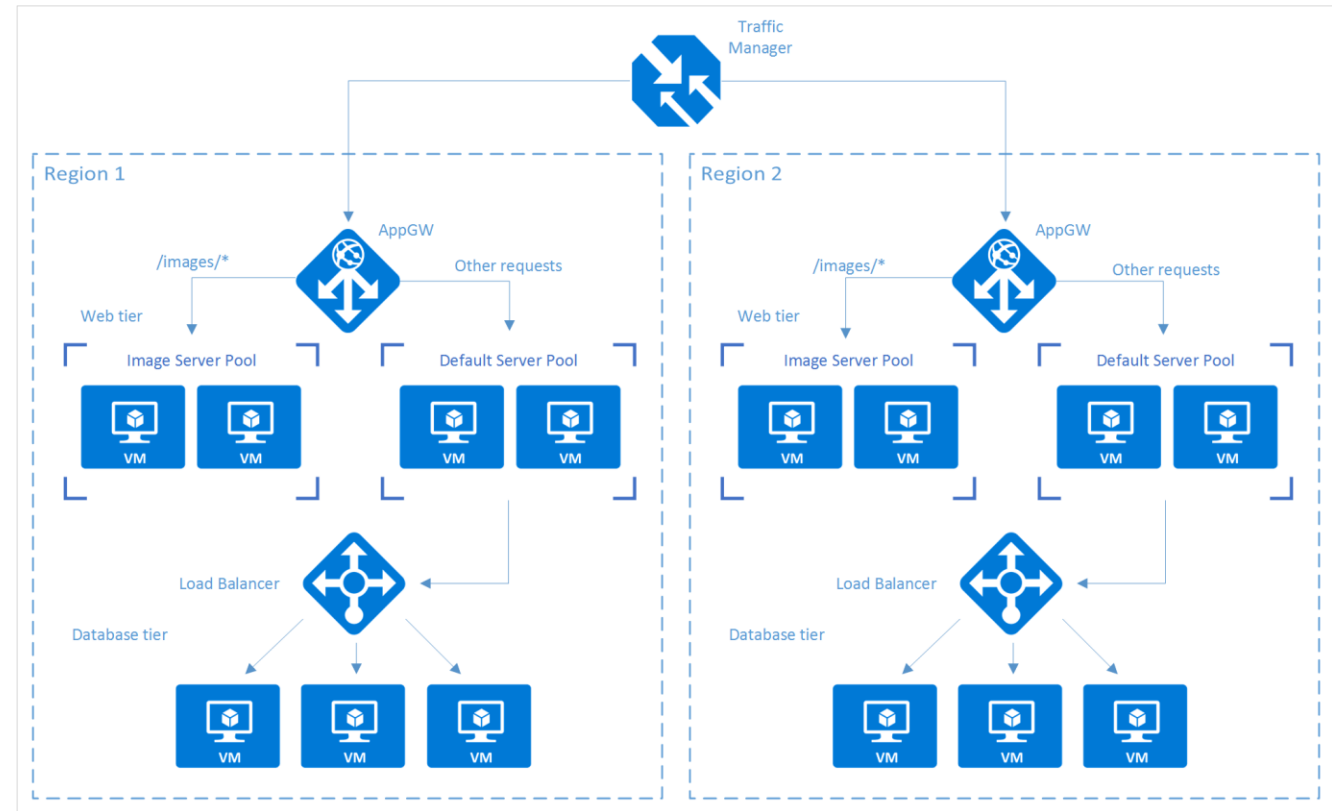
- 온-프레미스와 VNET S2S



BGP Protocol 사용

Azure 부하 분산기

Azure 서비스	정의	예제
트래픽 관리자	지역간 리디렉션과 가용성	http://news.com → apac.news.com → emea.news.com → us.news.com
Azure 부하 분산기	지역내 확장성 및 가용성	emea.news.com → AppGw1 → AppGw2 → AppGw2
Azure 애플리케이션 게이트웨이	URL/콘텐츠 기반 라우팅 및 부하 분산	news.com/topnews news.com/sports news.com/images
VM	웹 서버	IIS, Apache, Tomcat

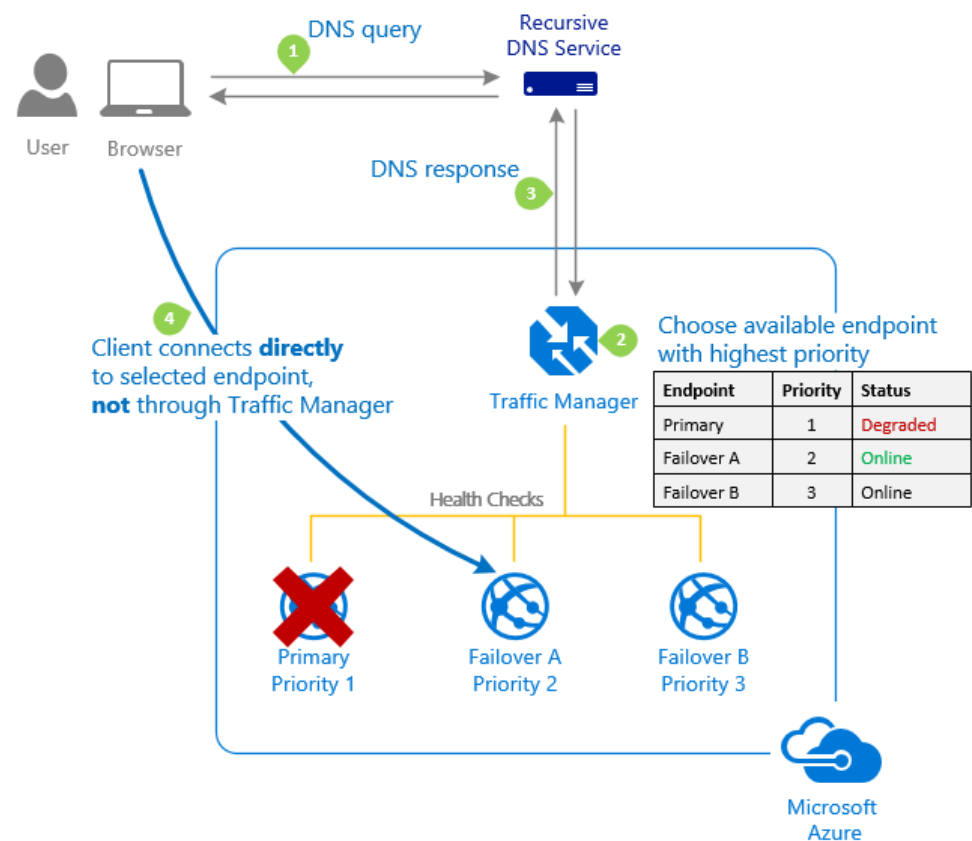


Azure 트래픽 관리자

- 트래픽을 DNS에 기반하여 전 세계 Azure 지역 서비스에 분산하는 부하 분산 장치

- 트래픽 라우팅 방법

- 우선 순위
- 가중치
- 성능
- 지리적

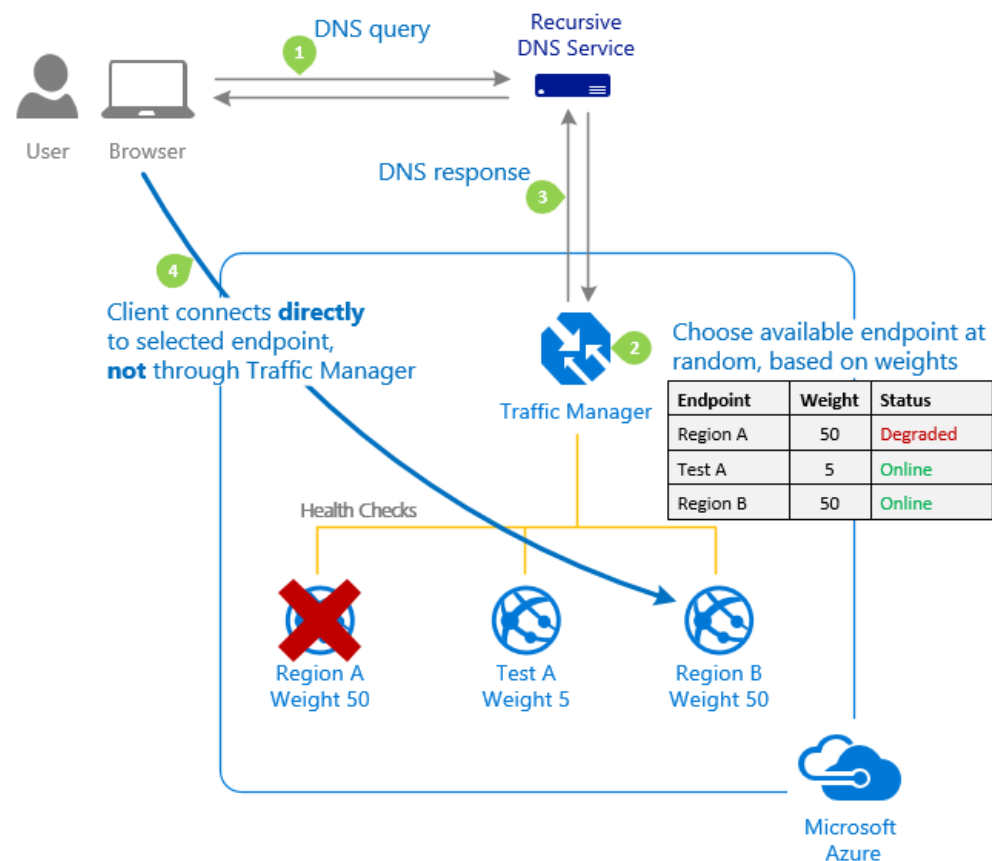


Azure 트래픽 관리자

- 트래픽을 DNS에 기반하여 전 세계 Azure 지역 서비스에 분산하는 부하 분산 장치

- 트래픽 라우팅 방법

- 우선 순위
- 가중치
- 성능
- 지리적

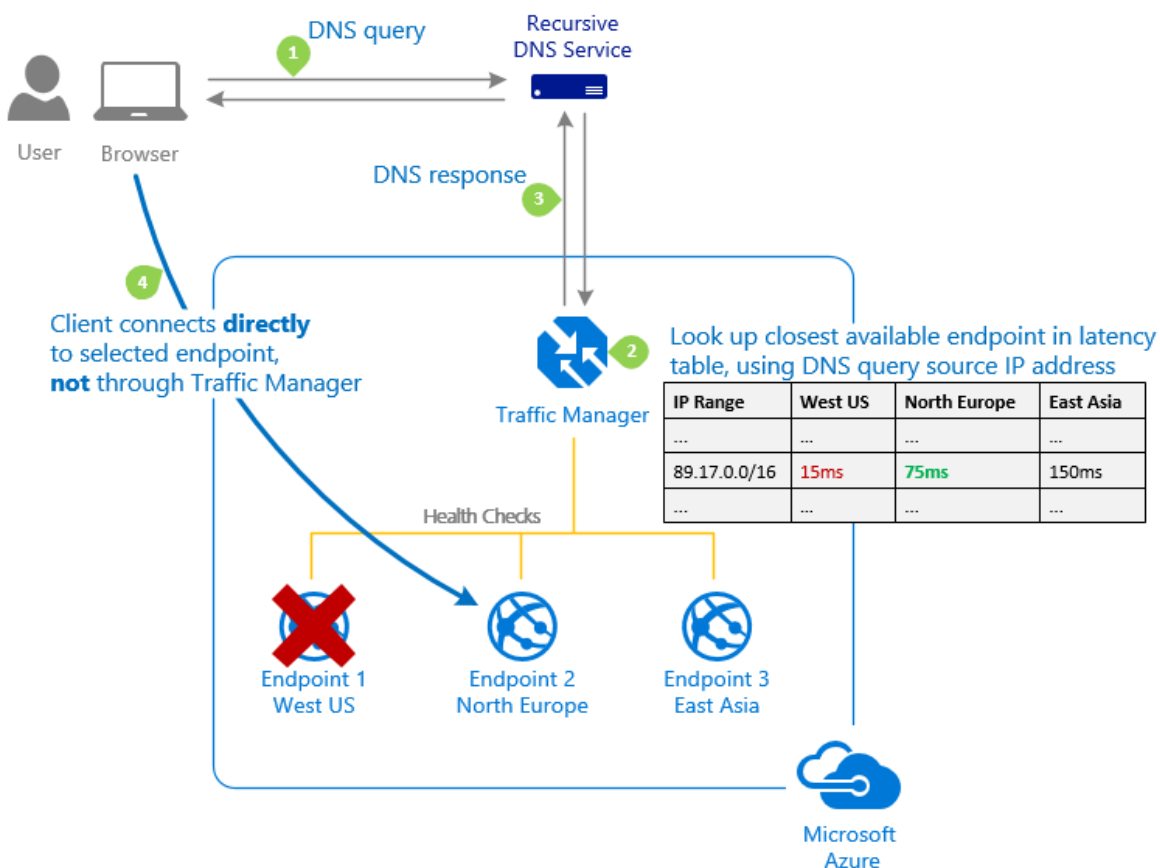


Azure 트래픽 관리자

- 트래픽을 DNS에 기반하여 전 세계 Azure 지역 서비스에 분산하는 부하 분산 장치

- 트래픽 라우팅 방법

- 우선 순위
- 가중치
- 성능
- 지리적

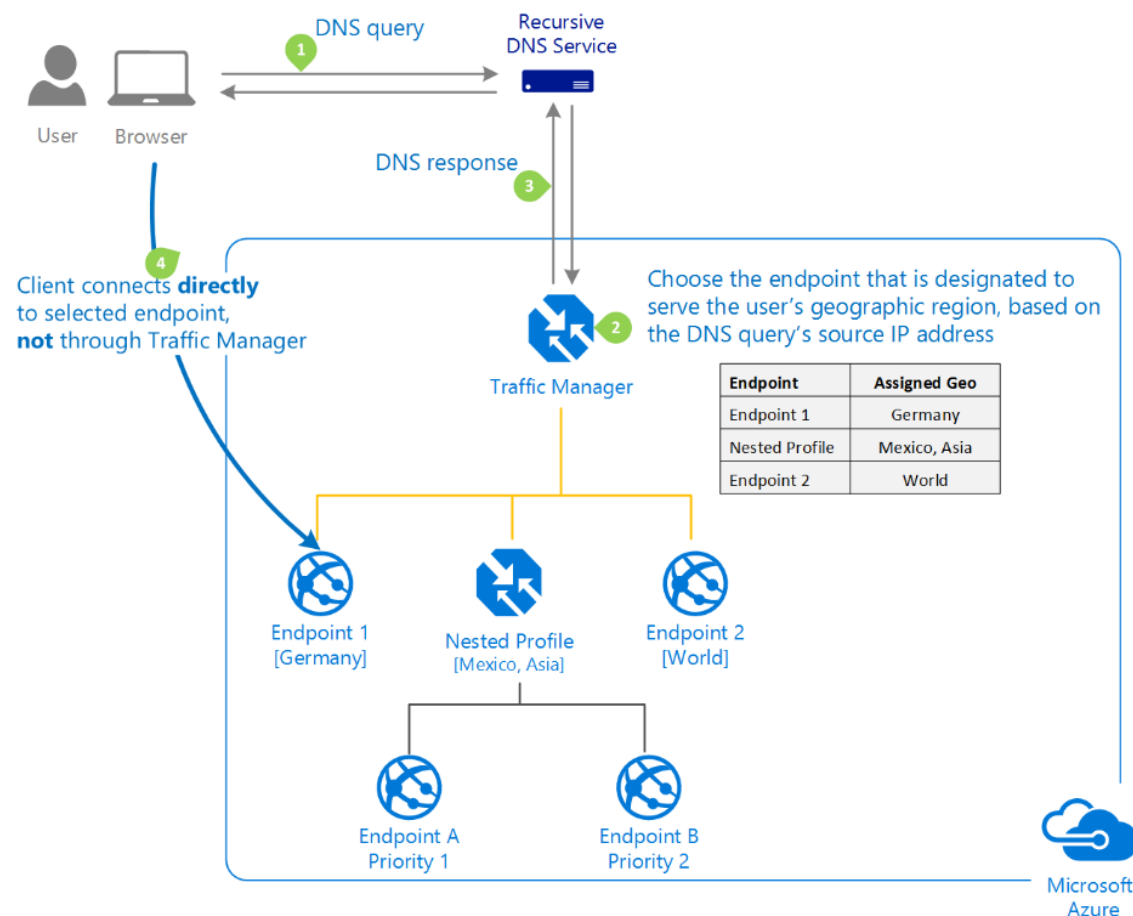


Azure 트래픽 관리자

- 트래픽을 DNS에 기반하여 전 세계 Azure 지역 서비스에 분산하는 부하 분산 장치

- 트래픽 라우팅 방법

- 우선 순위
- 가중치
- 성능
- 지리적



Azure 트래픽 관리자

- 트래픽을 DNS에 기반하여 전 세계 Azure 지역 서비스에 분산하는 부하 분산 장치
- 엔드포인트 모니터링 옵션
 - 엔드포인트에 GET 요청 수행. 200-OK 혹은 상태 코드 * 범위에서 결과가 반환된다면 정상 간주

jepttm - 구성
Traffic Manager 프로필

검색(Ctrl+F) < 저장 취소

라우팅 방법
성능

* DNS TTL(Time to Live)
60 초

엔드포인트 모니터링
프로토콜
HTTP

* 포트
80

* 경로
/

사용자 지정 헤더 설정
host.contoso.com ✓

상태 코드 범위가 필요합니다(기본값: 200).
200-299 ✓

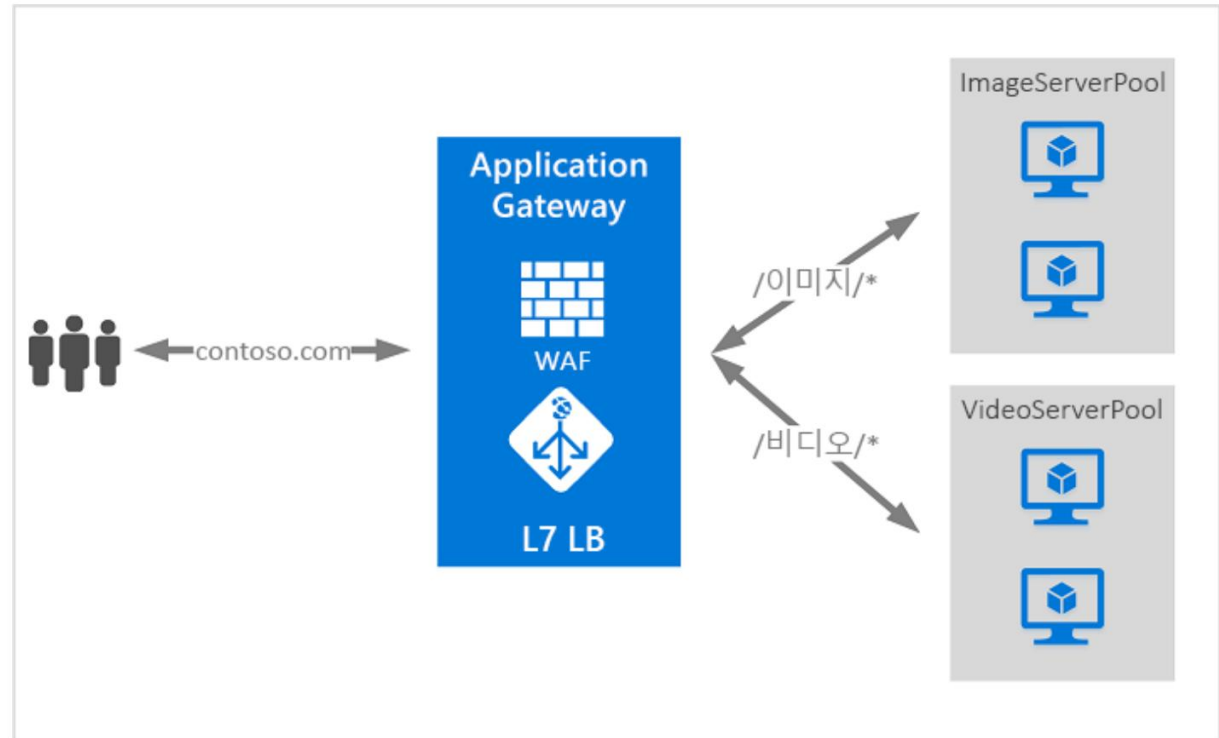
빠른 엔드포인트 장애 조치(failover) 설정
프로브 간격
30 초

* 허용되는 오류 수
3

* 프로브 시간 제한
10 초

애플리케이션 게이트웨이

- 웹 응용 프로그램에 대한 트래픽을 관리할 수 있도록 하는 웹 트래픽 부하 분산 장치
- 보안
 - SSL 종료
 - SSL 프로토콜 버전 허용/거부
- 세션 및 사이트 관리
 - 쿠키 기반
- 콘텐츠 관리
 - URL 기반 라우팅
- 백엔드 관리
 - 로그
 - 상태 프로브
- 자동 크기 조정 [미리보기]



애플리케이션 게이트웨이

- Azure 화면

대시보드 > KC-PT-RG > KC-PT-AG - 구성

KC-PT-AG - 구성

애플리케이션 게이트웨이

검색(Ctrl+/)

- 개요
- 활동 로그
- 액세스 제어(IAM)
- 태그
- 문제 진단 및 해결

설정

- 구성**
- 웹 애플리케이션 방화벽
- 백 엔드 풀
- HTTP 설정
- 프론트 엔드 IP 구성
- 수신기
- 규칙
- 상태 프로브
- 속성
- 잠금
- 자동화 스크립트

저장 취소

* 계층 ⓘ

표준

* SKU 크기 ⓘ

중형

* 인스턴스 수 ⓘ

2

* HTTP2

사용 안 함 사용

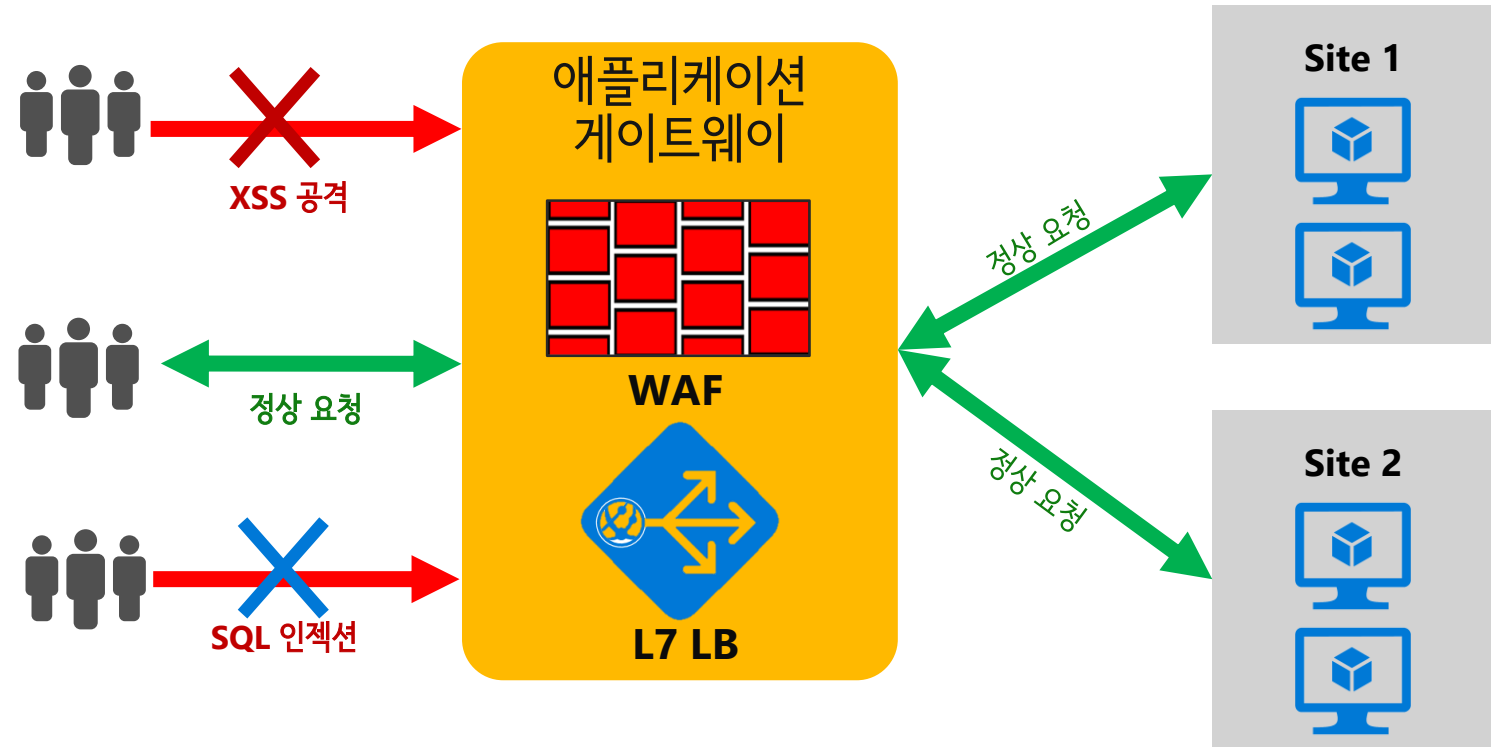
애플리케이션 게이트웨이 –WAF(Web Application Firewall)

- 보안

- 웹 기반 침입 감지
- Core Rule Set

- 사전 구성

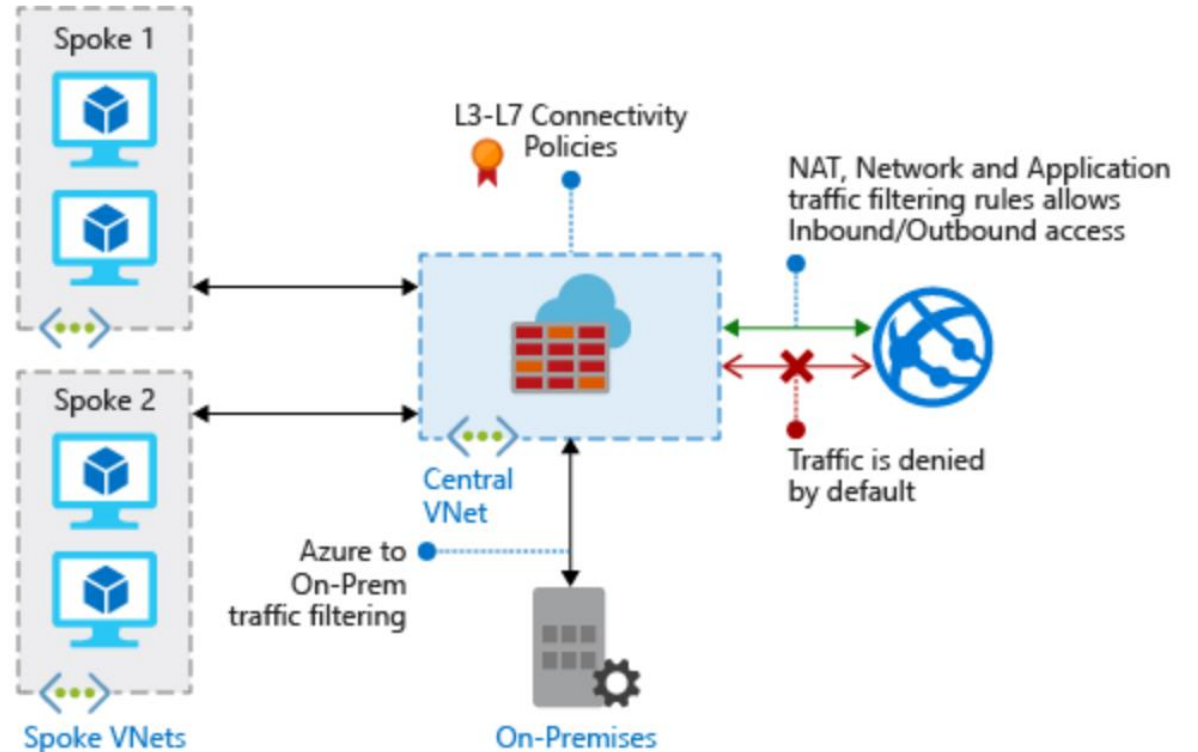
- 웹 기반 침입 감지
- 상위 10개의 웹 취약점에 대한 OWASP* 코어 규칙 3.0/2.2.9
 - SQL 인젝션
 - XSS 공격
 - 등등



애플리케이션 게이트웨이 DEMO

Azure Firewall

- Azure Virtual Network 리소스를 보호하는 관리되는 클라우드 기반 네트워크 보안 서비스
- 고가용성, 확장성
- 규칙 – 가상 네트워크 전반에 규칙 적용
 - NAT 규칙 컬렉션
 - 네트워크 규칙 컬렉션
 - 애플리케이션 규칙 컬렉션

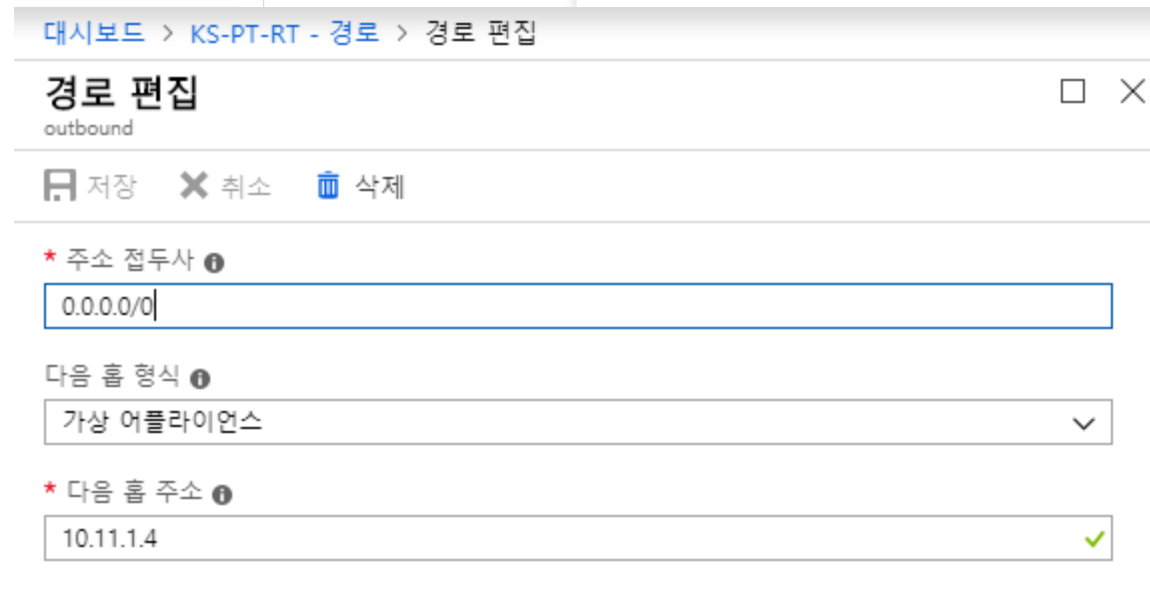


Azure Firewall –데모 화면

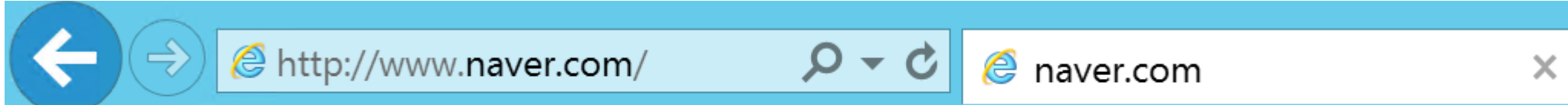
- Azure Firewall 설정



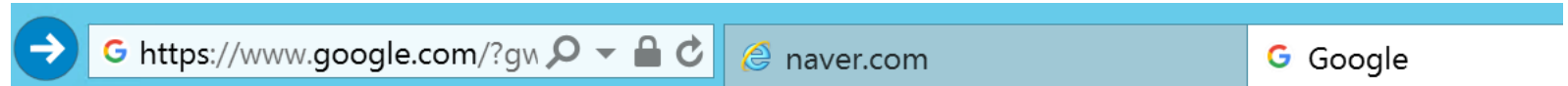
- 경로 테이블 설정



Azure Firewall –데모 화면



HTTP request from 10.11.2.4:50778 to www.naver.com:80. Action: Deny. No rule matched. Proceeding with default action



Google

Google 검색

I'm Feeling Lucky

Google 제공 서비스: [English](#)

Azure Firewall DEMO

감사합니다.